Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

SYMMETRIC FUNCTIONS FORMED BY SYSTEMS OF ELEMENTS OF A FINITE ALGEBRA AND THEIR CONNECTION WITH FERMAT'S QUOTIENT AND BERNOULLI'S NUMBERS.*

By H. S. Vandiver.

In a number of different investigations in the theory of numbers we encounter expressions formed by symmetric functions of systems of integers selected from a set $1, 2, \cdots, m$. I give a few known examples. We have the Wilson theorem:

$$(p-1)! \equiv -1 \pmod{p},$$

when p is prime. From the Lagrange congruence

$$(x-1)(x-2)\cdots(x-(p-1)) \equiv x^{p-1}-1 \pmod{p},$$

we find that the elementary symmetric functions formed by the integers $1, 2, \cdots, p-1$, and of dimension less than $p-1$, are all divisible by p.

Sylvester, in his study of Fermat's quotient, arrived at a formula which was given in the following form by Mirimanoff,†

$$q(m) \equiv \sum_{n=1}^{p-1} \frac{x_n}{p-n} \pmod{p},$$

where

$$q(m) = \frac{m^{p-1}-1}{p},$$

$$x_n \equiv \frac{n}{p} \pmod{m} \qquad (0 < x_n \leqq m).$$

This relation may be written

$$q(m) \equiv \sum_{n=1}^{m} x_n C_n \pmod{p},$$

where

$$C_k = \sum_i (mi+k)^{p-2},$$

and i ranges so that $mi+k$ represents all the integers of this form which are less than p. Note that the C's consist of symmetric functions formed by systems of integers in arithmetical progression selected from the set $1, 2, \cdots, p-1$.

Kronecker‡ in his investigation of the divisibility of the first factor of

---

[*] Presented to the American Mathematical Society at New York, April, 1913, and April, 1916,

[†] Crelle, vol. 115.

[‡] Cf. Hilbert, Die Theorie der Algebraischen Zahlkörpers, p. 430.

the class number of a cyclotomic field, defined by $\theta = e^{\frac{2i\pi}{l}}$, by the prime l, encountered relations from which we may derive the following:

$$\sum_i q_i r^{i(2t-1)} \equiv \frac{(r^{2t}-1)b_{2t}}{2tr^{2t-1}} \pmod{l},$$

where

$$t < \frac{l-1}{2}, \qquad q_i = \frac{rr_i - r_{i+1}}{l},$$

r being a primitive root of l, $b_1 = -\frac{1}{2}$, $b_{2a+1} = 0$, $b_{2a} = (-1)^{a+1}B_a$, $a > 0$. The B's are the numbers of Bernoulli and r_i is the least positive residue of r^i, modulo l.

In an article on Fermat's last theorem* the writer has derived from a theorem due to Frobenius the relation

$$\frac{b_a(1-k^a)}{a} \equiv \sum_{i=1}^{k-1} \frac{f_a(\alpha^i)}{1-\alpha^{il}} \pmod{l},$$

for $1 < a < l-1$, α a primitive kth root of unity, $f_a(\alpha^i) = \sum_{r=1}^{l-1} r^{a-1}\alpha^{ir}$, and $1 < k < l$. In the present paper, a few theorems will be given which serve as a basis for deriving as special cases all the results mentioned above as well as some generalizations.

Symmetric functions in a general finite algebra.

1. A finite algebra† is defined as a finite set of elements which may be combined by addition, subtraction and multiplication, subject to the commutative, associative, and distributive laws of ordinary algebra, such that the sum, difference or product of any two elements is uniquely determined as an element of the set, and in which also occurs an element playing the rôle of unity under multiplication. It is shown that every algebra of this type contains a set of m elements called integral elements. The integer m is called the base of the algebra A. Consider a set of elements in A, say

$$n_1, n_2, \cdots, n_k,$$

which has the property that there exists in A an element n (not unity) such that

$$nn_1, nn_2, \cdots, nn_k,$$

is a permutation of the original set. Such a system will be termed a *conjugate set* in the finite algebra A. The number n will be referred to as a multiplier of the set.

---

[*] Crelle, vol. 144, p. 314.

[†] Vandiver, Transactions Amer. Math. Society, vol. 13, p. 293.

Consider an I.H.S.F. (integral homogeneous symmetric function) formed by a conjugate set, say

$$S(n_1, n_2 \cdots n_k).$$

By definition of n, we have

$$S(nn_1, nn_2, \cdots, nn_k) = S = n^d S,$$

and

$$(n^d - 1)S = 0, \tag{1}$$

d being the dimension of the function S. Now if it is possible to select n and d so that $n^d - 1$ is a unit in A, then $S = 0$. This can be done in a number of special cases. We have, if t is the totient of A,*

$$n^t = 1$$

in the algebra. Assume that n and $n - 1$ are units in A, and that d is prime to t. Then it may be shown that $n^d - 1$ is a unit in A. For if $n^d - 1 \equiv 0 \pmod{N}$, where N is a non unit, then we also have

$$n^t - 1 \equiv 0 \pmod{N}.$$

If n belongs to the exponent e modulo N, then $t \equiv 0 \pmod{e}$, as is easily seen, and also $d \equiv 0 \pmod{e}$. Hence, since d is prime to t, we have $e = 1$, but this gives $n - 1 \equiv 0 \pmod{N}$, contrary to definition. Hence $n^d - 1$ is a unit and we have from (1),

Theorem I. *Any* I.H.S.F. *formed by the elements of a conjugate set in a finite algebra A, whose degree is prime to the totient of A, is zero in A, provided there exists a multiplier n of the set such that $n(n - 1)$ is a unit in A.*

Symmetric functions of systems of residues of an ideal modulus.

2. A complête system of residues with respect to an ideal modulus represents a finite algebra. We shall consider this type of algebra in detail with regard to symmetric functions. A C.S.U.R. (complete system of unit residues) modulo $\mathfrak{m}$, an ideal in an algebraic field Ω, is reproduced if each element of the system is multiplied by an integer ρ in Ω which is prime to $\mathfrak{m}$.†

Let

$$\mathfrak{m} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_k^{a_k},$$

where the $\mathfrak{p}$'s are distinct prime ideals in Ω, and let S be an I.H.S.F. of the C.S.U.R. modulo $\mathfrak{m}$. Multiplication by ρ gives (if d is the degree of S) $\rho^d S$, and also S, modulo $\mathfrak{m}$. Hence

$$S(\rho^d - 1) \equiv 0 \pmod{\mathfrak{m}}. \tag{1a}$$

---

* Vandiver, Transactions Amer. Math. Society, vol. 13, p. 294.

† Dirichlet-Dedekind, Zahlentheorie (4th edition), p. 570.

Now assume that d is not a multiple of $\varphi(\mathfrak{p}_1)$, where $\varphi(\mathfrak{p}_1)$ represents the indicator of $\mathfrak{p}_1$, and let ρ_1 be a primitive root of $\mathfrak{p}_1$. Then

$$d = r\varphi(\mathfrak{p}_1) + d_1,$$

where $0 < d_1 < \varphi(\mathfrak{p}_1)$, and we have

$$\rho_1^{d_1} \not\equiv 1 \pmod{\mathfrak{p}_1}.$$

Similarly we may select algebraic integers ρ_s such that

$$\rho_s^d \not\equiv 1 \pmod{\mathfrak{p}_s}, \qquad s = 2, 3, \cdots, k,$$

provided that d is a multiple of none of the integers $\varphi(\mathfrak{p}_s)$. Now there is an algebraic integer ρ_m in Ω such that*

$$\rho_m \equiv \rho_1 \pmod{\mathfrak{p}_1}, \qquad \rho_m \equiv \rho_2 \pmod{\mathfrak{p}_2}, \qquad \cdots, \qquad \rho_m \equiv \rho_k \pmod{\mathfrak{p}_k}.$$

Then $\rho_m{}^d - 1$ is prime to each of the ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$, and is therefore prime to $\mathfrak{m}$. In (1a) put $\rho = \rho_m$, then $S \equiv 0 \pmod{\mathfrak{m}}$. Whence the following

Theorem II. *If we form an* I.H.S.F. *with the algebraic integers of a* C.S.U.R. *of an ideal modulus* $\mathfrak{m}$, *in an algebraic field* Ω, *then the resulting integer is divisible in* Ω *by* $\mathfrak{m}$, *unless the dimension of the function is divisible by one of the integers* $\varphi(\mathfrak{p}_s)$, $s = 1, 2, \cdots, k$, *where* $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$ *are the distinct ideal prime factors of* $\mathfrak{m}$.

The theorem holds also if we replace the C.S.U.R. by the complete system of incongruent residues modulo $\mathfrak{m}$.

3. Consider an I.H.S.F. formed by all the unit elements of any finite algebra A of dimension d, and let n be an integral mark of A. Let n_g be a primitive root of p_g, where m, the base of A, is

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Let

$$n = \sum_{\epsilon=1}^{r} \left(\frac{m}{p_\epsilon^{\alpha_\epsilon}} \right)^{\phi(p_\epsilon^{\alpha_\epsilon})} n_\epsilon,$$

$\varphi(k)$ being the indicator of k, and put

$$d \equiv f_\epsilon \pmod{\overline{p_\epsilon - 1}}, \qquad \text{where} \qquad f_\epsilon < p_\epsilon - 1.$$

Then unless one of the f's is zero, we see that $n^d - 1$ is prime to each of the integral marks $p_1, p_2, \cdots, p_r$. Consequently $n^d - 1$ is a unit in A, and from (1), $S = 0$. Whence the†

---

* Dirichlet-Dedekind, l. c., page 568.

† This method was used by Hensel to prove the theorem for the case of a system of integers 1, 2, $\cdots$, $p - 1$, modulo p, a prime. Cf. Kronecker, Vorlesungen über Zahlentheorie, vol. I, page 104, with reference to Hensel on page 498.

Theorem III. *An I.H.S.F. formed by all the unit elements of a finite algebra A vanishes in A except when the dimension of the function is divisible by one of the integers* $p_k - 1$, *where* $k = 1, 2, \cdots, r$, *and* $p_1, p_2, \cdots, p_r$ *are the distinct prime factors of the base of A.*

This theorem also holds if we replace the set of *unit* elements by the set of *all* the elements, as is easily seen.

4. We examine now the special finite algebra formed by the elements of a Galois field of order p^n. If θ is any element of the field which belongs to the exponent a, then the elements $\theta, \theta^2, \cdots, \theta^a$ form a group under multiplication which will be termed a sub-group in the field. By familiar methods it is possible to exhibit all the distinct elements of the field, other than zero, by the rectangular array

$$\begin{array}{llll} \omega_1, & \omega_1\theta, & \cdots & \omega_1\theta^{a-1} \\ \omega_2, & \omega_2\theta, & \cdots & \omega_2\theta^{a-1} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \omega_b, & \omega_b\theta, & \cdots & \omega_b\theta^{a-1} \end{array} \tag{2}$$

where $ab = p^n - 1$. Consider an I.H.S.F. (which involves only ath powers) of the elements $\omega_1, \omega_2, \cdots, \omega_b$ of degree ad, say $S(\omega_1{}^a, \omega_2{}^a, \cdots, \omega_b{}^a)$. Further let i be a primitive root in the Galois field. Then

$$S((i\omega_1)^a, (i\omega_2)^a, \cdots, (i\omega_b)^a) = i^{ad}S(\omega_1{}^a, \omega_2{}^a, \cdots, \omega_b{}^a).$$

We have from (2)

$$(i\omega_k)^a = (\theta^s\omega_l)^a = \omega_l{}^a,$$

where s is some integer less than a. As k ranges over the set $1, 2, \cdots, b$, then l ranges over the same set. For otherwise we would have $(i\omega_k)^a = (i\omega_{k_1})^a$, whence $\omega_k = \theta^t\omega_{k_1}$, where $t < a$, contrary to the definition of (2). Hence in the field

$$S((i\omega_1), (i\omega_2)^a, \cdots (i\omega_b)^a) = S = i^{ad}S, \qquad (i^{ad} - 1)S = 0,$$

which gives $S = 0$, unless

$$i^{ad} - 1 = 0,$$

i. e., unless $ad \equiv 0$, (mod $p^n - 1$), since i is a primitive root in the field. This gives the

Theorem IV. *If we form a rectangular array of the elements (not zero) of a Galois field of order* p^n *with respect to a sub-group in the field of order a, then an I.H.S.F. involving only the ath powers of all the multipliers in the array is zero in the field unless the dimension d of the function is a multiple of* $(p^n - 1)/a$.

Considering the special case in which the Galois field is represented by a complete set of residues modulo p, and putting $a = 2$, we obtain the corollary: *Any I.H.S.F. formed by the system of odd incongruent residues of* p, *which involves only squares of these residues, is divisible by* p, *unless the degree of said function with respect to said squares is a multiple of* $(p - 1)/2$, *where* p *is prime.*

Symmetric functions of residues of a rational modulus.

5. Examine now a complete system of residues with respect to a rational integer $m(\neq 2)$ as modulus. Consider a conjugate set in the algebra so formed and let it be represented by

$$n_1, n_2, \cdots, n_k, \qquad (n_i < m), \tag{3}$$

where k is the order of the set. Let n be any unit multiplier of the set (not unity), then the integers

$$\frac{y_a m + n_a}{n} \qquad (a = 1, 2, \cdots, k),$$

$$y_a \equiv -\frac{n_a}{m} \pmod{n} \qquad (0 \leqq y_a < n),$$

are identical with those of the set (3). For, modulo m, they reduce to n_a/n $(a = 1, 2, \cdots, k)$, which set reduces to (3) modulo m, since $1/n = n^{t-1}$ is a multiplier of the conjugate set, t being the totient of the algebra. Further, each is less than m, since y_a by hypothesis is less than n. Now form any I.H.S.F., say S, of the integers in (3) of degree i. We have

$$S(n_1, \cdots) = S\left(\frac{y_1 m + n_1}{n}, \cdots\right),$$

$$n^i S(n_1, \cdots) = S(y_1 m + n_1, \cdots). \tag{4}$$

Consider a particular term of $S(y_1 m + n_1, \cdots)$, say

$$(y_a m + a)(y_b m + b) \cdots (y_h m + h),$$

where $a, b, \cdots h$ are certain of the n's, not necessarily distinct, and i in number. This may be written

$$ab \cdots h\left(\frac{y_a}{a} m + 1\right)\left(\frac{y_b}{b} m + 1\right) \cdots \left(\frac{y_h}{h} m + 1\right),$$

and expanding in powers of m this becomes

$$abc \cdots h\left(1 + m\left[\frac{y}{ab \cdots h}\right]_1 + m^2\left[\frac{y}{ab \cdots h}\right]_2 \cdots + m^i\left[\frac{y}{ab \cdots h}\right]_i\right),$$

where

$$\left[\frac{y}{ab\cdots h}\right]_s$$

represents the elementary symmetric function formed from

$$\frac{y_a}{a},\ \frac{y_b}{b},\ \cdots,\ \frac{y_k}{k}$$

taken s at a time.

Then by (4)

$$n^i S = \sum_{a,\,b\,\ldots\,h}\ \sum_{s=1}^{i} ab\cdots h\left(1 + m^s\left[\frac{y}{ab\cdots h}\right]_s\right),$$

where the outside summation is effected by replacing $ab\cdots h$ by all the terms of the function $S(n_1\cdots)$ in turn. This relation may be written

$$\frac{(n^i - 1)S}{m} = \sum_{ab\,\ldots\,h}\ \sum_{s=0}^{i-1} ab\cdots h m^s\left[\frac{y}{ab\cdots h}\right]_{s+1}. \tag{5}$$

We now proceed to set down a number of consequences of this theorem. Put $i = k$, $S = \prod_{r=1}^{k} n_r$, and divide through by S, then*

$$\frac{n^k - 1}{m} = \sum_{s=0}^{k-1} m^s\left[\frac{y}{n_1 n_2\cdots n_k}\right]_{s+1}. \tag{6}$$

Modulo m, this assumes the form, provided the conjugate set includes units only,

$$\frac{n^k - 1}{m} \equiv \sum_{r=1}^{k}\frac{y_r}{n_r} \pmod{m}. \tag{6a}$$

Letting $m = p$, a prime, and $k = p - 1$, with $n = 2$, and reducing the relation (6) modulo p^2, we obtain

$$q(2) \equiv 1 + \frac{1}{3} + \cdots + \frac{1}{p-2} + pP \pmod{p^2}, \tag{7}$$

where P is the elementary symmetric function of the elements

$$1,\ \frac{1}{3},\ \cdots\ \frac{1}{p-2}$$

taken two at a time. Setting

$$S_a = 1 + \frac{1}{3^a} + \cdots + \frac{1}{(p-2)^a},$$

---

* This theorem includes as special cases most of the results of Sylvester, Comptes Rendus, vol. 52, 1861, p. 161; Mirimanoff, Crelle, vol. 115, 1895, p. 295; Baker, Proceedings of the London Mathematical Society, ser. 2, vol. IV, p. 131.

we have evidently

$$S_1^2 = S_2 + 2P.$$

By the corollary to Theorem IV we have, if $p > 3$,

$$S_2 \equiv 0 \pmod{p},$$

whence

$$S_1^2 \equiv 2P \pmod{p}.$$

From (7) we have

$$q(2) \equiv S_1 + p\frac{S_1^2}{2} \pmod{p^2} \qquad (p > 3),$$

which shows that

$$q(2) \equiv 0 \pmod{p^2}$$

if and only if

$$1 + \frac{1}{3} + \cdots + \frac{1}{p-2} \equiv 0 \pmod{p^2}.$$

Now in (5) put $S = 1^i + 2^i + \cdots + (p-1)^i$, where $m = p$. Then

$$\text{(7a)} \qquad \frac{(n^i - 1)S}{p} = \sum_{a=1}^{p-1} \sum_{s=1}^{i} a^i \binom{i}{s} \left(\frac{y_a}{a}\right)^s p^{s-1},$$

and, modulo p, this becomes, if n is any of the integers $2, 3, \cdots p-1$,

$$\frac{(n^i - 1)S}{ip} \equiv \sum_{a=1}^{p-1} y_a a^{i-1} \pmod{p}.$$

It is known that

$$1^i + 2^i + \cdots + (p-1)^i \equiv b_i p \pmod{p^2},$$

where

$$b_1 = -\tfrac{1}{2}, \qquad b_{2a+1} = 0, \qquad b_{2a} = (-1)^{a-1}B_a,$$

$B_1 = \frac{1}{6}$, $B_2 = \frac{1}{30}$, etc., being the numbers of Bernoulli, and $i < p - 1$. Then

$$\text{(8)} \qquad \frac{(n^i - 1)b_i}{i} \equiv \sum_{a=1}^{p-1} y_a a^{i-1} \pmod{p}.$$

6. We now introduce roots of unity and derive some new relations involving them.

Let x be an indeterminate. Then if we set

$$(x - 1)F(x) = x^n - 1,$$

we have

$$(x - 1)\frac{dF}{dx} + F = nx^{n-1}.$$

Letting $x = \alpha^{hm}$, where $\alpha = e^{2i\pi/n}$, and multiplying by $\alpha^{hn_a + hm}$, we may write, n being prime to m,

$$\frac{\alpha^{hn_a}}{\alpha^{hm} - 1} = \frac{\sum_{s=1}^{n-1} s\alpha^{h(ms + n_a)}}{n},$$

if h is an integer not divisible by n. We have

$$\sum_{s=1}^{n-1} s\alpha^{h(ms+n_a)} = \sum_{s_1} s_1\alpha^{h(ms_1+n_a)} + s_2,$$

where s_1 ranges over those integers less than n such that $ms_1 + n_a \not\equiv 0 \pmod{n}$, and

$$s_2 \equiv -\frac{n_a}{m} \pmod{n} \qquad (n > s_2 \geqq 0).$$

Then we obtain

$$\sum_{h=1}^{n-1}\sum_{s=1}^{n-1} s\alpha^{h(ms+n_a)} = \sum_{s_1}\sum_{h=1}^{n-1} s_1\alpha^{h(ms_1+n_a)} + (n-1)s_2.$$

The right-hand member of the above relation reduces to

$$-\frac{n(n-1)}{2} + ns_2,$$

which gives

$$\sum_{h=1}^{n-1}\frac{\alpha^{hn_a}}{\alpha^{hm}-1} + \frac{n-1}{2} = s_2 = y_a, \tag{9}$$

as previously defined. Letting $m = p$, a prime, and substituting in (7a) we obtain

$$\frac{(n^i-1)S}{p} = \sum_{a=1}^{p-1}\sum_{s=1}^{i} p^{s-1}a^{i-s}\binom{i}{s}\left(\sum_{h=1}^{n-1}\frac{\alpha^{ah}}{\alpha^{hp}-1} + \frac{n-1}{2}\right)^s.$$

Modulo p, this becomes $(i < p - 1)$,

$$\frac{(n^i-1)b_i}{i} \equiv \sum_{h=1}^{n-1}\frac{f_i(\alpha^h)}{\alpha^{hp}-1} \pmod{p},$$

where the f function has the form defined previously. Applying (9) to (6a), we have

$$\frac{n^k-1}{m} \equiv \sum_{h=1}^{n-1}\frac{f_0^{(n)}(\alpha^h)}{\alpha^{hm}-1} + \frac{n-1}{2}\sum_a\frac{1}{n_a} \pmod{m},$$

n_a ranging over all the elements of the conjugate set and

$$f_0^{(n)}(\alpha) = \sum_a n_a^{-1}\alpha^{n_a}.$$

If $n - 1$ is prime to m, then Theorem I gives

$$\frac{n^k-1}{m} \equiv \sum_{h=1}^{n-1}\frac{f_0^{(n)}(\alpha^h)}{\alpha^{hm}-1} \pmod{m}. \tag{10}$$

7. If we rearrange the right-hand member of (8) by collecting like values of y_a, we may write this member as follows:

$$\sum_{c=1}^{n-1}(n-c)\left\{\left(cp-\left[\frac{(c-1)p}{n}\right]n-n\right)^{i-1}+\left(cp-\left[\frac{(c-1)p}{n}\right]n-2n\right)^{i-1}\right.$$
$$\left.+\cdots+\cdots+\left(cp-\left[\frac{cp}{n}\right]n\right)^{i-1}\right\}.$$

Reduce this expression modulo p and divide the result by $(-n)^{i-1}$. The term in the reduced form corresponding to $c = 1$ has the form

$$(n-1)\left(1^{i-1}+2^{i-1}+\cdots+\left[\frac{p}{n}\right]^{i-1}\right).$$

Similarly the term for $c = 2$ is

$$(n-2)\left\{\left(\left[\frac{p}{n}\right]+1\right)^{i-1}+\left(\left[\frac{p}{n}\right]+2\right)^{i-1}+\cdots+\left[\frac{2p}{n}\right]^{i-1}\right\}.$$

The sum of the last two expressions may be written

$$\sum_{k=1}^{[p/n]} k^{i-1}+(n-2)\sum_{k_1=1}^{[2p/n]} k_1^{i-1}.$$

In the same way the sum of the expressions for $c = 1$, 2, and 3 takes the form

$$\sum_{k=1}^{[p/n]} k^{i-1}+\sum_{k_1=1}^{[2p/n]} k_1^{i-1}+(n-3)\sum_{k_2=1}^{[3p/n]} k_2^{i-1}.$$

Proceeding in this manner we obtain finally

$$(11)\qquad \frac{(1-n^i)b_i}{in^{i-1}} \equiv \sum_{u=1}^{n-1}\sum_{k=1}^{[up/n]} k^{i-1} \pmod{p}.$$

Put $m = p$ in (6a) and let the n's range over 1, 2, $\cdots$, $p - 1$. Then applying the above process we find

$$(12)\qquad -nq(n) \equiv \sum_{u=1}^{n-1}\sum_{k=1}^{[up/n]} \frac{1}{k} \pmod{p}.$$

Set $(n + 1)$ for n in this relation and subtract; we then obtain

$$-nq(n)+(n+1)q(n+1) \equiv \Sigma\frac{1}{h} \pmod{p},$$

where h ranges over the integers which satisfy

$$\frac{\beta p}{n+1} < h < \frac{\beta p}{n},$$

$\beta = 1, 2, \cdots, n$. From (11) we obtain in a similar way

$$(13)\qquad \frac{b_i(n^{p-i}-(n+1)^{p-i}+1)}{i} \equiv \Sigma h^{i-1} \pmod{p},$$

a relation due to Kummer* for i even.

---

* Abhandlungen der K. Akad. der Wiss. zu Berlin, 1857.